

International Association of Risk and Compliance Professionals (IARCP)  
 1200 G Street NW Suite 800, Washington DC, 20005-6705 USA  
 Tel: 202-449-9750, Web: [www.risk-compliance-association.com](http://www.risk-compliance-association.com)



*Monday, May 22, 2023*

Top 10 risk and compliance related news stories and world events that (for better or for worse) shaped the week's agenda, and what is next

Dear members and friends,

An *offline* payment with CBDC is a transfer of value between devices, that does not require connection to any ledger system, often in the absence of internet or telecoms connectivity. A user device may be online (connected to the internet), but still disconnected from a ledger system.



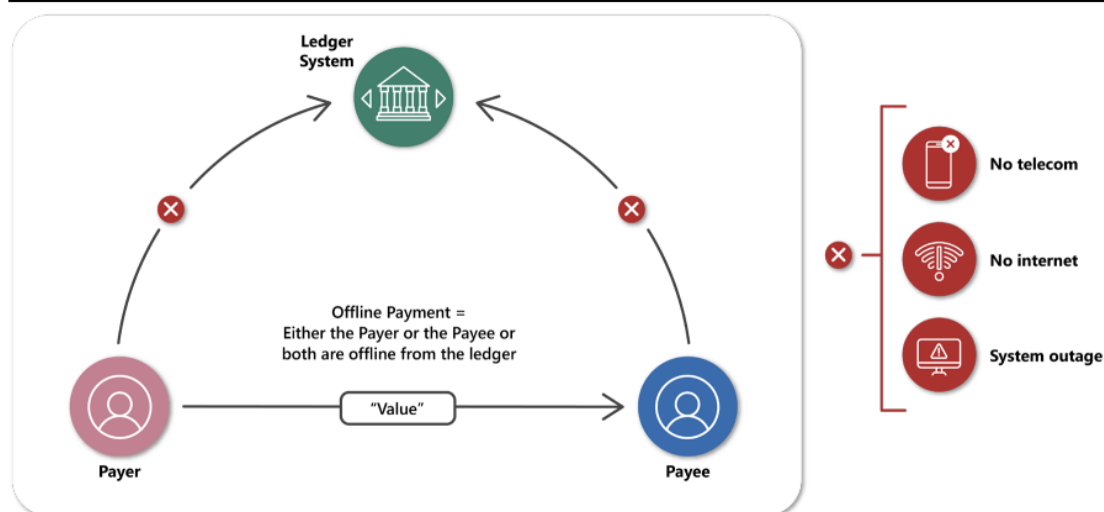
This is an interesting definition, in the new paper with title “Project Polaris: - Offline payments with CBDC” from the Bank for International Settlements (BIS). The paper is intended to help central banks to:

- understand the available technologies and *security* measures;
- understand the main *threats, risks and risk management* measures;
- understand the *privacy* issues, inclusion needs and resilience options;
- understand the design and architecture principles involved; and
- gain perspective on potential *operational and change management*

issues.

### Offline payments and ledger systems

Figure 1



In CBDC systems, *risk management by design* is key. This is particularly important for CBDC systems that provide offline payments functionality, as offline payment solutions are exposed to *different threats and vulnerabilities*, and therefore different risks, than online solutions.

We have a new paper, and some interesting definitions in this context:

- A *risk* refers to the potential for destruction, damage or loss of business assets and data resulting from a threat.
- A *threat* is an event that unintentionally or intentionally exploits a vulnerability to damage, destroy or obtain an asset.
- A *vulnerability* is a weakness in networks, hardware, software or processes which a threat actor exploits to damage, destroy or obtain an asset.

Risk types can be categorised as:

- *Technology risks* – the risk that any technology failure will disrupt an entity's business or operations.
- *Operational risks* – the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.
- *Reputational risks* – the risk of reputational damage to an entity when it

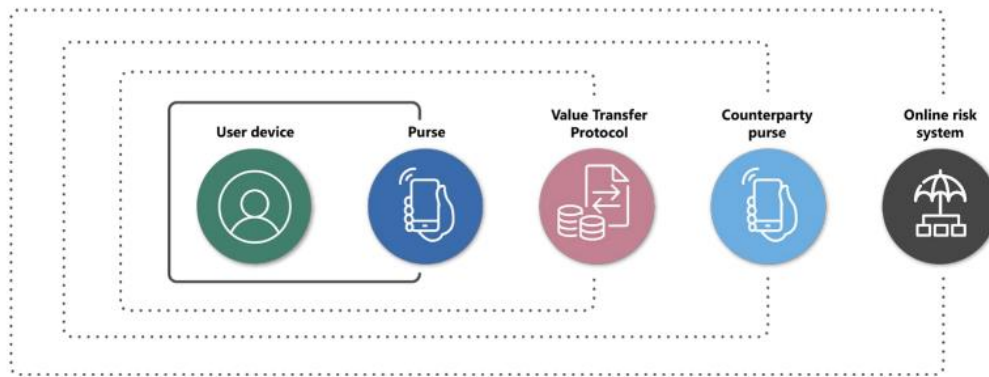
fails to meet the expectations of its stakeholders and this is negatively perceived.

Risks can belong to one or more of the categories above. Each would need to be carefully assessed and mitigated through either technical or non-technical risk management measures or a combination of both, with some element of residual risk that would have to be deemed acceptable to the organisation.

There are surprises in the paper too: “There may be other kinds of risk in connection with offline payments, for example *legal risks*, that are out of scope of the handbook. The degree of risk each presents may vary by country, capabilities, infrastructure and solution used.”

A simplified view of the layers of risk management components

Figure 8



Read more at number 3 below. Welcome to the Top 10 list.

*Best regards,*

*George Lekatis*

George Lekatis  
 President of the IARCP  
 1200 G Street NW Suite 800,  
 Washington DC 20005, USA  
 Tel: (202) 449-9750  
 Email: [lekatis@risk-compliance-association.com](mailto:lekatis@risk-compliance-association.com)  
 Web: [www.risk-compliance-association.com](http://www.risk-compliance-association.com)  
 HQ: 1220 N. Market Street Suite 804,  
 Wilmington DE 19801, USA  
 Tel: (302) 342-8828

*Number 1 (Page 6)***PCAOB Enhances Transparency of Inspection Reports With New Section on Auditor Independence and More**

Eight 2022 inspection reports released today include new transparency enhancements

*Number 2 (Page 8)***European Court of Justice (CJEU), requirements under which data subjects affected by a breach of the GDPR can claim for compensation of non-material damages under Art. 82 GDPR**

**InfoCuria**  
Case-law

*Number 3 (Page 12)***Project Polaris: secure and resilient CBDC systems, offline and online***Number 4 (Page 17)***PCAOB Releases 2022 Inspection Reports for Mainland China, Hong Kong Audit Firms**

Chair Williams says reports are “a powerful first step toward accountability,” as demand for complete access continues

*Number 5 (Page 21)***The evolving nature of banking, bank culture, and bank runs**

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the 21st Annual Symposium on "Building the Financial System of the 21st Century - an agenda for Europe and the United States", sponsored by Harvard Law School, Program on International Financial Systems, Frankfurt am Main.



## *Number 6 (Page 26)*

### Green Swan 2023: Climate transition in the real economy: what should central banks know about it?

A virtual conference co-organised by the Bank for International Settlements, the Central Bank of Chile, the Network for Greening the Financial System and the South African Reserve Bank.



## *Number 7 (Page 28)*

### Responsible Cyber Power in Practice



## *Number 8 (Page 30)*

### New Sensors With the HOTS for Extreme Missions

Sensors are everywhere – except in harsh environments too hot for key components. DARPA's new HOTS program looks to change that



## *Number 9 (Page 32)*

### Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service



## *Number 10 (Page 37)*

### Hunting Russian Intelligence “Snake” Malware





*Number 1*

## PCAOB Enhances Transparency of Inspection Reports With New Section on Auditor Independence and More

Eight 2022 inspection reports released today include new transparency enhancements



The Public Company Accounting Oversight Board (PCAOB) announced it has enhanced its inspection reports with a new section on auditor independence and a range of other improvements that increase transparency by making publicly available more information that is relevant, reliable, and useful for investors and other stakeholders.

The changes will appear in reports for PCAOB inspections completed in 2022, beginning with eight reports released today, which can be found at the Firm Inspection Reports page.

“We are committed to making our inspection reports as valuable as possible for investors, audit committees, and others, and today we take another significant step in advancing that goal by shining a greater light on independence violations and more,” said PCAOB Chair Erica Y. Williams. “These enhancements will provide relevant information that investors have asked for and support improvements in overall audit quality.”

The enhanced inspection reports will include:

1. *A new section of the report focused on independence violations:* Reports will feature a new independence section (Part I.C) that will discuss instances of noncompliance with PCAOB rules related to maintaining independence, as well as potential noncompliance with U.S. Securities and Exchange Commission independence rules.
2. *More information related to fraud procedures and the identification and assessment of the risks of material misstatements:* Reports will expand Part I.B to include deficiencies related to AS 2401, Consideration of Fraud in a Financial Statement Audit, and AS 2110, Identifying and Assessing Risks of Material Misstatement.
3. *More commentary:* Reports will provide additional commentary in Part I.A for certain situations, such as whether the audit was the firm’s first audit of the issuer or whether the firm had identified significant risks, including fraud, for areas in which PCAOB inspection staff identified deficiencies.

4. *New graphs:* For annually inspected firms, reports will include charts to clearly show firm and engagement partner tenure.

“These enhancements will further drive audit quality and make our inspection reports even more useful for the public,” said George R. Botic, Director of the PCAOB’s Division of Registration and Inspections. “We are especially pleased to provide more information on auditor independence, which is essential to audit quality and underpins the objectivity, credibility, and integrity of the audit.”

Learn more about PCAOB inspection reports and the inspection process at our Inspections page, at: <https://pcaobus.org/oversight/inspections>



The screenshot shows the PCAOB website's 'Firm Inspection Reports' page. The header includes the PCAOB logo (Public Company Accounting Oversight Board) and navigation links for About, Oversight, Resources, and News & Events. A breadcrumb trail reads 'Home > Oversight > Inspections'. The main heading is 'Firm Inspection Reports'. Below this, the text states: 'The Sarbanes-Oxley Act authorizes the PCAOB to inspect registered firms for the purpose of assessing compliance with certain laws, rules, and professional standards in connection with a firm's audit work for public companies, other issuers, and broker-dealer clients.' It further explains that registered firms with 100 or fewer audit reports are inspected every three years, while those with more than 100 are inspected annually. A note at the bottom indicates that the page focuses on issuer audits, with a link to a dedicated page for broker-dealer inspections.

To read more:

<https://pcaobus.org/news-events/news-releases/news-release-detail/pcao-b-enhances-transparency-of-inspection-reports-with-new-section-on-audit-or-independence-and-more>



*Number 2***European Court of Justice (CJEU), requirements under which data subjects affected by a breach of the GDPR can claim for compensation of non-material damages under Art. 82 GDPR****InfoCuria**  
Case-law**JUDGMENT OF THE COURT**

Reference for a preliminary ruling – Protection of natural persons with regard to the processing of personal data – Regulation (EU) 2016/679 – Article 82(1) – Right to compensation for damage caused by data processing that infringes that regulation – Conditions governing the right to compensation – Mere infringement of that regulation not sufficient – Need for damage caused by that infringement – Compensation for non-material damage resulting from such processing – Incompatibility of a national rule making compensation for such damage subject to the exceeding of a threshold of seriousness – Rules for the determination of damages by national courts.

The dispute in the main proceedings and the questions referred for a preliminary ruling

11 From 2017, Österreichische Post, a company incorporated under Austrian law, an address broker, collected information on the political affinities of the Austrian population. Using an algorithm that takes into account various social and demographic criteria, it defined ‘target group addresses’. The data thus generated were sold to various organisations, to enable them to send targeted advertising.

12 In the course of its activity, Österreichische Post processed data which, by way of statistical extrapolation, led it to infer that the applicant in the main proceedings had a high degree of affinity with a certain Austrian political party. That information was not communicated to third parties, but the applicant in the main proceedings, who had not consented to the processing of his personal data, felt offended by the fact that an affinity with the party in question had been attributed to him.

The fact that data relating to his supposed political opinions were retained within that company caused him great upset, a loss of confidence and a feeling of exposure. It is apparent from the order for reference that no harm other than those adverse emotional effects of a temporary nature has been established.



13 In that context, the applicant in the main proceedings brought an action before the Landesgericht für Zivilrechtssachen Wien (Regional Court for Civil Matters, Vienna, Austria) seeking, first, an injunction for Österreichische Post to cease processing the personal data in question and, second, an order requiring that company to pay him the sum of EUR 1 000 by way of compensation for the non-material damage which he claims to have suffered. By decision of 14 July 2020, that court upheld the application for an injunction but rejected the claim for compensation.

14 On appeal, the Oberlandesgericht Wien (Higher Regional Court, Vienna, Austria) confirmed, by judgment of 9 December 2020, the decision at first instance. As regards the claim for compensation, that court referred to recitals 75, 85 and 146 of the GDPR and held that the Member States' provisions of national law on civil liability supplement the provisions of that regulation, in so far as the latter does not contain special rules. In that regard, it noted that, under Austrian law, a breach of the rules on the protection of personal data is not automatically associated with non-material damage and gives rise to a right to compensation only where such damage reaches a certain 'threshold of seriousness'. In its view, that is not the case with regard to the negative feelings which the applicant in the main proceedings has invoked.

15 Hearing the action brought by the two parties in the main proceedings, the Oberster Gerichtshof (Supreme Court, Austria), by interim judgment of 15 April 2021, did not uphold the appeal on a point of law brought by Österreichische Post against the injunction imposed on it. Therefore, only the appeal on a point of law which the applicant in the main proceedings brought against the rejection of his claim for compensation which had been raised against him remains before that court.

16 In support of its request for a preliminary ruling, the referring court states that it is apparent from recital 146 of the GDPR that Article 82 of that regulation established its own rules on liability for the protection of personal data, which superseded the rules in force in the Member States. Therefore, the concepts contained in Article 82, in particular the concept of 'damage' referred to in paragraph 1 thereof, should be interpreted autonomously and the conditions for the implementation of that liability should be defined in the light not of the rules of national law, but of the requirements of EU law.

17 Specifically, in the first place, as regards the right to compensation for a breach of personal data protection, that court tends to consider, in the light of the sixth sentence of recital 146 of the GDPR, that compensation based on Article 82 of that regulation presupposes that material or non-material damage has actually been suffered by the data subject. It

argues that the award of such compensation is subject to proof of specific damage distinct from that breach, which does not in itself establish the existence of non-material damage. In its view, recital 75 of that regulation refers to the mere possibility that non-material damage may result from the breaches listed therein and, although recital 85 refers to the risk of a 'loss of control' of the data affected, that risk is, however, uncertain in the present case, since those data were not transmitted to a third party.

18 In the second place, as regards the assessment of the compensation that may be awarded under Article 82 of the GDPR, that court considers that the principle of effectiveness of EU law must have a limited impact, on the grounds that that regulation already provides for severe penalties for breaches thereof and that it is therefore not necessary to award a high level of compensation in addition to ensure its effectiveness. In its view, any compensation due on that basis must be proportionate, effective and dissuasive, so that the damages awarded may fulfil a compensatory function, but not be punitive in nature, which is extraneous to EU law.

19 In the third place, the referring court questions the argument put forward by Österreichische Post that the award of such compensation is subject to the condition that the breach of personal data protection has caused particularly serious harm. In that regard, it notes that recital 146 of the GDPR advocates a broad interpretation of the concept of 'damage' within the meaning of that regulation. It takes the view that non-material damage must be compensated, under Article 82 of that regulation, if it is tangible, even if it is minor. By contrast, such damage should not be compensated if it appears to be completely negligible, as would be the case for the merely unpleasant feelings that are typically associated with such a breach.

20 In those circumstances, the Oberster Gerichtshof (Supreme Court) decided to stay the proceedings and to refer the following questions to the Court of Justice for a preliminary ruling:

(1) Does the award of compensation under Article 82 of [the GDPR] also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?

(2) Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?

(3) Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a

consequence [or effect] of the infringement of at least some weight that goes beyond the upset caused by that infringement?’

*The Court (Third Chamber) hereby rules:*

1. Article 82(1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) **must be interpreted as meaning that the mere infringement of the provisions of that regulation is not sufficient to confer a right to compensation.**
2. Article 82(1) of Regulation 2016/679 **must be interpreted as precluding a national rule or practice which makes compensation for non-material damage, within the meaning of that provision, subject to the condition that the damage suffered by the data subject has reached a certain degree of seriousness.**
3. Article 82 of Regulation 2016/679 **must be interpreted as meaning that for the purposes of determining the amount of damages payable under the right to compensation enshrined in that article, national courts must apply the domestic rules of each Member State relating to the extent of financial compensation, provided that the principles of equivalence and effectiveness of EU law are complied with.**

To read more:

<https://curia.europa.eu/juris/document/document.jsf?text=&docid=273284&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4947438>



*Number 3***Project Polaris: secure and resilient CBDC systems, offline and online**

This handbook provides a comprehensive overview of the key aspects of offline payments with CBDC and is intended to serve as a guide for central banks considering implementing offline payments capabilities.

In this handbook, an offline payment is defined as a transfer of value (CBDC) between devices that takes place without requiring connection to any ledger system.

This could be due to a system outage or in the absence of internet or telecommunications connectivity.

A survey conducted by the BIS Innovation Hub as part of the development of this handbook shows that 49% of central banks surveyed consider offline payments with retail CBDC to be vital, while another 49% deemed it to be advantageous.

Providing offline payments with CBDC is an important requirement for many central banks, but its implementation is complex and involves a number of technology, security and operational considerations that need to be planned and designed for at the earliest possible stages.

These considerations have implications on decisions related to policy, ecosystem roles and responsibilities, design, architecture, security, technology, investment, ongoing operations, change management and risk management.

The research for this handbook has found there is no one-size-fits-all solution, with each country having multiple reasons for providing offline payments with CBDC.

The types and suitability of solutions for offline payments will vary by country depending on local requirements.

This handbook provides some of the main reasons and usage scenarios for offline payments; a map and an explanation of the technology components; and a set of design criteria for risk management, privacy, inclusion and resilience.

It also provides a set of considerations that central banks can use to inform their planning, policy development, technology and business requirements, procurement activities and future operations.

This handbook is intended to help central banks to:

- understand the available technologies and security measures;
- understand the main threats, risks and risk management measures;
- understand the privacy issues, inclusion needs and resilience options;
- understand the design and architecture principles involved; and
- gain perspective on potential operational and change management issues.

Project Polaris: - Offline payments with CBDC

×



Project Polaris: - Offline payments with CBDC

×





## Contents

<b>Acronyms, abbreviations and definitions</b>	<b>7</b>
<b>1. Executive summary</b>	<b>13</b>
<b>2. Introduction</b>	<b>16</b>
<b>3. Offline payments with CBDC</b>	<b>19</b>
3.1 Reasons for offline payments with CBDC	19
3.2 Modes of offline payment	22
3.3 Key lessons from history relevant to offline payments with CBDC	26
<b>4. Offline payment solutions for CBDC</b>	<b>28</b>
4.1 Logical architecture for offline payment solutions	28
4.2 Tamper-resistant user devices	30
4.2.1 Secure element (SE)-based	31
4.2.2 Trusted execution environment (TEE)-based	32
4.2.3 Secure software-based	32
4.3 User onboarding	33
4.4 Provisioning and life cycle management	34
4.4.1 Secure provisioning processes	34
4.4.2 Cryptographic key generation processes	35
4.4.3 Lifecycle management activities	35
4.6 Offline risk management	37
4.6.1 Risk parameter management	37
4.6.2 Transaction history management	37
4.6.3 Limiting the lifetime or uses of cryptographic keys	38
4.6.4 Block list management	38
4.7 Purses	38
4.8 Value transfer protocol	39
4.9 Value-form	40
4.10 Online updates	41
4.11 Value transfer mechanism	41
4.12 Interoperability	42

---

4.12.1	Between different offline solutions	42
4.12.2	Between online and offline solutions	43
<b>5.</b>	<b>Risk management by design</b>	<b>45</b>
5.1	Key assumptions	46
5.2	Threats and vulnerabilities	46
5.2.1	Counterfeiting via physical breaches	46
5.2.2	Counterfeiting via cryptographic protocol analysis (cryptanalysis)	47
5.2.3	Side-channel attacks	47
5.2.4	Fault-inducing attacks	47
5.2.5	Cryptography strength, lifetime and ability to update	48
5.2.6	Master cryptographic key compromise	48
5.2.7	Third-party device compromise	48
5.3	Risks	49
5.3.1	Device obsolescence	49
5.3.2	Double-spending	49
5.3.3	Fraud	49
5.3.4	Lost value	50
5.3.5	Third-party vendors and supply chains	51
5.3.6	Lack of risk management and breach detection	52
5.3.7	Complexity of the technology stack	52
5.3.8	Insider threats	52
5.4	Risk management measures	52
5.5	Technology risk management	53
5.5.1	General criteria	54
5.5.2	Measures to mitigate the risk of counterfeiting	55
5.5.3	Measures to mitigate side-channel attacks	56
5.5.4	Measures to mitigate crypto-durability and crypto-agility risks	56
5.5.5	Measures to mitigate risks of master cryptographic key compromise	56
5.5.6	Measures to mitigate risks from third-party device compromise	57
5.5.7	Measures to mitigate risks from obsolescence	57
5.5.8	Measures to mitigate double-spending risks	58
5.5.9	Measures to mitigate fraud risks	58
5.5.10	Measures to mitigate third-party vendor and supply chain risks	60

5.5.11 Measures to mitigate lack of real-time transaction monitoring and breach detection	61
5.6 Operational risk management	63
5.7 Reputational risk management	64
<b>6. Privacy by design</b>	<b>66</b>
6.1 Privacy principles	66
6.2 Privacy considerations for offline payments with CBDC	67
<b>7. Inclusion by design</b>	<b>70</b>
7.1 Inclusion considerations	70
7.2 Supporting multiple ways to pay	73
<b>8. Resilience by design</b>	<b>75</b>
8.1 Short-term resilience	75
8.2 Ongoing resilience	75
8.3 Civil contingency resilience	76
8.4 Resilience considerations	76
8.5 Design considerations to improve resilience	77
<b>9. Conclusion</b>	<b>79</b>

To read more: <https://www.bis.org/about/bisih/topics/cbdc/polaris.htm>

<https://www.bis.org/publ/othp64.pdf>



*Number 4***PCAOB Releases 2022 Inspection Reports for Mainland China, Hong Kong Audit Firms**

Chair Williams says reports are “a powerful first step toward accountability,” as demand for complete access continues



Public Company Accounting Oversight Board (PCAOB) Chair Erica Y. Williams made the following statement today after the PCAOB released inspection reports for two firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.

INSPECTION REPORT

**KPMG Huazhen LLP**

COUNTRY      INSPECTION REPORT DATE

China      Mar. 28, 2023

 [Download PDF](#)

INSPECTION REPORT

**PricewaterhouseCoopers**

COUNTRY      INSPECTION REPORT DATE

Hong Kong      Mar. 28, 2023

 [Download PDF](#)
*From Chair Williams:*

Thanks to the leadership of the U.S. Congress in passing the Holding Foreign Companies Accountable Act (HFCAA), last year, the PCAOB secured complete access to inspect registered public accounting firms headquartered in mainland China and Hong Kong for the first time in history.

Today, the PCAOB is releasing the inspection reports for both firms inspected in 2022: KPMG Huazhen LLP in mainland China and PricewaterhouseCoopers in Hong Kong.

Both reports show unacceptable rates of Part I.A deficiencies, which are deficiencies of such significance that PCAOB staff believe the audit firm failed to obtain sufficient appropriate audit evidence to support its work on the public company’s financial statements or internal control over financial reporting.

The PCAOB inspected a total of eight engagements in 2022 – four at each of the two firms – including the types of engagements to which People’s Republic of China (PRC) authorities had previously denied access, such as large state-owned enterprises and issuers in sensitive industries.

PCAOB inspectors found Part I.A deficiencies in 100% (four of four) of the audit engagements reviewed at KPMG Huazhen and 75% (three of four) of the audit engagements reviewed for PwC Hong Kong.

As I have said before, any deficiencies are unacceptable. At the same time, it is not unexpected to find such high rates of deficiencies in jurisdictions that are being inspected for the first time. And the deficiencies identified by PCAOB staff at the firms in mainland China and Hong Kong are consistent with the types and number of findings the PCAOB has encountered in other first-time inspections around the world.

The fact that our inspectors found these deficiencies is a sign that the HFCAA was effective and the inspection process worked as it is supposed to. We identified problems so now we can begin the work of holding firms accountable to fix them.

Today’s reports are a powerful first step toward accountability. By shining a light on deficiencies, our inspection reports provide investors, audit committees, and potential clients with important information so they can make informed decisions and hold firms accountable. And the power of transparency applies public pressure for firms to improve.

The remediation process is another tool we use to hold firms accountable for fixing deficiencies. By law, public inspection reports do not initially include quality control deficiencies that inspectors find. Instead, firms have one year to remediate those deficiencies. If they don’t remediate those deficiencies to the Board’s satisfaction, we make them public.

Finally, where appropriate, our inspectors will refer inspection findings to our enforcement team for possible action. If violations are found, our enforcement staff will not hesitate to recommend sanctions, including imposing significant money penalties and barring bad actors from performing future audits.

Last year was only the beginning of our work to inspect and investigate firms in mainland China and Hong Kong.

Our enforcement teams continue to pursue investigations, and inspectors have begun fieldwork for 2023’s inspections. We anticipate fieldwork will



continue off and on throughout most of the year, which is common practice for inspections such as these in jurisdictions around the world.

The two firms we inspected in 2022 audited 40% of the total market share of U.S.-listed companies audited by Hong Kong and mainland China firms, and we are on track to hit 99% of the total market share by the end of this year. So, there is no question that the PCAOB is prioritizing inspections that are the most relevant to investors on U.S. markets – because protecting investors is what this is all about.

Indeed, the release of today's reports is yet another sign that investors are more protected because of Congress' leadership in passing the HFCAA. And last year's legislation, which shortened the timeline from three years to two years, provided important leverage as the PCAOB continues demanding complete access to inspect and investigate firms headquartered in mainland China and Hong Kong – with no loopholes and no exceptions.

As I have said before, should PRC authorities obstruct or otherwise fail to facilitate the PCAOB's access – in any way and at any time – the Board will act immediately to consider the need to issue a new determination.

I want to thank the hardworking inspectors, investigators, and PCAOB staff who continue this important work on behalf of investors every day.



THIS IS A PUBLIC VERSION OF A PCAOB INSPECTION REPORT

PORTIONS OF THE COMPLETE REPORT ARE OMITTED FROM THIS DOCUMENT IN ORDER TO COMPLY WITH SECTIONS 104(g)(2) AND 105(b)(5)(A) OF THE SARBANES-OXLEY ACT OF 2002

PCAOB RELEASE NO. 104-2023-049



# 2022 Inspection PricewaterhouseCoopers

(Headquartered in Hong Kong Special  
Administrative Region of the People's Republic  
of China)

March 28, 2023

THIS IS A PUBLIC VERSION OF A PCAOB INSPECTION REPORT

PORTIONS OF THE COMPLETE REPORT ARE OMITTED FROM THIS DOCUMENT IN ORDER TO COMPLY WITH SECTIONS 104(g)(2) AND 105(b)(5)(A) OF THE SARBANES-OXLEY ACT OF 2002



PCAOB RELEASE NO. 104-2023-050

To read more:

<https://pcaobus.org/news-events/news-releases/news-release-detail/pcaob-releases-2022-inspection-reports-for-mainland-china-hong-kong-audit-firms>

<https://pcaobus.org/oversight/inspections/firm-inspection-reports>



*Number 5***The evolving nature of banking, bank culture, and bank runs**

Michelle W Bowman, Member of the Board of Governors of the Federal Reserve System, at the 21st Annual Symposium on "Building the Financial System of the 21st Century - an agenda for Europe and the United States", sponsored by Harvard Law School, Program on International Financial Systems, Frankfurt am Main.



It is a pleasure to be with you here today. This symposium, focused on building the financial system of the twenty-first century, is very timely. Given the recent banking system stress many are welcoming a fresh look at whether the Dodd-Frank era changes to the financial system and the approach to supervision and regulation have kept pace with the evolving nature of banking, the evolving culture of banking, and how the risks of bank runs today have evolved to be meaningfully different from what we've seen in the past.

While my remarks will largely focus on the United States, the lens through which regulators and policymakers should view these issues has some broader applicability and is worthy of an ongoing discussion.

I will begin by offering a few thoughts on U.S. monetary policy. At our most recent meeting last week, in light of the ongoing unacceptably high inflation, the Federal Open Market Committee (FOMC) increased the target range for the federal funds rate by 25 basis points.

With this increase, the FOMC has raised the federal funds rate by 5 percentage points since March of last year. These increases, combined with the runoff of our balance sheet, are having the desired effect of tightening financial conditions.

In my view, our policy stance is now restrictive, but whether it is sufficiently restrictive to bring inflation down remains uncertain.

Some signs of slowing in aggregate demand, lower numbers of job openings and more modest gross domestic product (GDP) growth indicate that we have moved into restrictive territory.

But inflation remains much too high, and measures of core inflation have remained persistently elevated, with declining unemployment and ongoing wage growth. And, as senior loan officers signaled beginning last summer, credit has continued to tighten. I expect this trend will continue given increased bank funding costs and reduced levels of liquidity.

While the U.S. banking and financial system remains sound and resilient, the recent failures of three U.S. banks with unique risk profiles have added to the uncertainty surrounding the economic outlook. This uncertainty is further complicated by stock price movements among regional banks.

Should inflation remain high and the labor market remain tight, additional monetary policy tightening will likely be appropriate to attain a sufficiently restrictive stance of monetary policy to lower inflation over time.

I also expect that our policy rate will need to remain sufficiently restrictive for some time to bring inflation down and create conditions that will support a sustainably strong labor market. Of course, the economic outlook is uncertain and our policy actions are not on a preset course.

I will consider the incoming economic and financial data during the intermeeting period and its implications for the economic outlook in determining my view of the appropriate stance of monetary policy.

I will look for signs of consistent evidence that inflation is on a downward path when considering future rate increases and at what point we will have achieved a sufficiently restrictive stance for the policy rate.

In my view, the most recent CPI and employment reports have not provided consistent evidence that inflation is on a downward path, and I will continue to closely monitor the incoming data as I consider the appropriate stance of monetary policy going into our June meeting.

My remarks today will address the recent bank failures in the United States and how the evolution of the banking industry has influenced and amplified bank deposit run risk.

I will then discuss supervision, regulation, bank management culture, and technology, and how each of these changes the dynamics of our approach to building a stronger and more resilient financial system.

Finally, I will close with my views on the importance of approaching the future in a deliberate, evidence focused, and thoughtful manner.

*The Evolving Context of Banking and Bank Failures*

Those who are involved in the business of banking will not find this shocking, but it is a fundamental fact that banking involves risk. It is inherent in, and foundational to, the business of banking: banks take demand deposits—a short-term liability—and make term loans—creating a long-term asset.

Absent this intentional risk-taking, banks could not play their indispensable role of credit provision in the economy. There are many other risks, with the specific risks that banks face today as varied as the wide range of bank business models.

The most fundamental banking risks include credit, concentration, interest rate, liquidity, cybersecurity, more recently operational risk and, of course, the risk of contagion.

Banking simply cannot work in its current and historical form without risk, so unless the goal is to change the nature of banking, the task of policymakers and regulators is not to eliminate risk from the banking system, but rather to ensure that risk is appropriately and effectively managed.

Fundamentally, this is the basis for the bank regulatory frameworks that exist around the world. In countries with well-functioning and appropriately regulated banking systems, banks serve an indispensable role in credit provision and economic stability.

The goal is to create and maintain a system that supports prudent banking practices, and results in the implementation of appropriate risk management.

No efficient banking system can eliminate all bank failures. But well-designed and well-maintained systems can limit bank failures and mitigate the harm caused by any that occur.

In practice, the "maintenance" of the bank regulatory and supervisory framework has often been challenging, in part because maintenance requires vigilance in responding to evolving circumstances and risks.

Lapses in this effort are revealed when something breaks, which could include fragilities resulting from the emergence of unidentified risks and financial stability threats; banking practices that expose shortcomings in the supervisory framework; or policymakers, regulators, and/or examiners



who have lost sight of the fundamental goal of encouraging prudent banking practices and appropriate risk management.

The need for maintenance of the U.S. bank regulatory and supervisory framework has come into stark relief with the failures of two large banks in March, followed by a third at the beginning of May. The future and current policy choices made in responding to these failures will have important consequences for the U.S. banking system.

Including the extent to which bank regulation will continue to drive banking activities from regulated banks and into shadow banks. While shoring up the resiliency of the banking sector is important, it is also important that we consider the consequences of any regulatory change.

Before discussing the direction of policy, I think it's imperative that we pause and consider where we are and what has changed.

### *The Failure of Silicon Valley Bank*

As financial services have evolved to meet the demands and expectations of sophisticated and wealthy businesses and individuals, risks inherent in the very nature of these services—instant accessibility and transferability of funds—created the potential for instability at an extensive and accelerated scale.

For Silicon Valley Bank in particular, while the run was ignited by traditional concerns, it was much faster than previous bank runs, was fueled by the most modern communication methods and social media, and was enabled through new technology that allows customers to move money on a scale and at a velocity not previously accessible directly to customers.

On Thursday, March 9, SVB experienced a deposit outflow of more than \$40 billion, and more than \$100 billion was anticipated in queue for outflow on Friday, March 10.

Let's consider this in comparison to past bank failures and the pace and size of deposit outflows. Prior to SVB, the largest bank failure in U.S. history was the failure of Washington Mutual, which experienced two periods of large deposit outflows, the first lasted 23 days with outflows of \$9.1 billion, and the second \$18.7 billion over 16 days.

In other bank failures resulting from deposit runs, deposits flowed out of the bank in significantly smaller volumes and over much longer time horizons than SVB experienced on March 9 and 10.

The recent bank runs have many familiar elements. SVB relied on funding from extremely large deposits of technology and health care sector firms, which were mostly uninsured (more than 95 percent) and held in transaction accounts.

In traditional banking, uninsured depositors have historically been exposed to credit risk on their bank deposits, which provides some incentive for them to impose market discipline on the bank, such as by discouraging excessive risk-taking.

As we were very recently reminded, a disproportionate percentage of uninsured depositors can also present risk, since they may have strong incentives to withdraw their funds at the slightest sign of actual or perceived bank stress. These dynamics and incentives are certainly not new but have featured prominently in past bank runs.

The most significant shift has been one of speed. This is where modern technology has played a significant role, both in facilitating the transfer of funds and in the access to, and expedited flow of, information among depositors.

To read more:

<https://www.federalreserve.gov/newsevents/speech/bowman20230512a.htm>



*Number 6***Green Swan 2023: Climate transition in the real economy: what should central banks know about it?**

A virtual conference co-organised by the Bank for International Settlements, the Central Bank of Chile, the Network for Greening the Financial System and the South African Reserve Bank.














The third edition of Green Swan Conference brings together a wide range of high-calibre policymakers, experts and practitioners from different sectors to discuss in more detail climate transition and the real economy.

Day 1 focuses on new technologies and scaling up already feasible solutions, day 2 on the macroeconomic implications of the transition.

Sessions will be livestreamed on this page. Join the conversation on social media with the hashtag #GreenSwanConference.

**Day 1: 31 May**

Opening event	
12:00 - 12:05	<b>Welcome remarks</b>  Luiz Pereira da Silva / BIS
12:05 - 12:30	<b>Opening address</b>  Ravi Menon / Monetary Authority of Singapore and NGFS
Session 1: Scaling up already feasible solutions	
13:00 - 15:00	<b>Presentations and panel discussion</b> <div style="display: flex; flex-wrap: wrap; justify-content: space-around;"> <div style="text-align: center;">  Doug Arent / National Renewable Energy Laboratory         </div> <div style="text-align: center;">  Georgina Grenon / Paris 2024 Organising Committee         </div> <div style="text-align: center;">  Suzi Kerr / Environmental Defense Fund         </div> <div style="text-align: center;">  James Thurlow / International Food Policy Research Institute         </div> </div>

Session 2: Developing new technologies	
15:30 -17:30	<p><b>Case studies and panel discussion</b></p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  <p>José Miguel Benavente / Corporación de Fomento de la Producción</p> </div> <div style="text-align: center;">  <p>Renaud Crassous / NUWARD, EDF Group</p> </div> </div> <div style="display: flex; justify-content: space-around; margin-top: 10px;"> <div style="text-align: center;">  <p>Paul Hugues / International Energy Agency</p> </div> <div style="text-align: center;">  <p>M Mercedes Maroto-Valer / Heriot-Watt University</p> </div> </div> <div style="margin-top: 10px;">  <p>Chair: Bertille Delaveau / Banque de France</p> </div>

To read more:

[https://www.bis.org/events/green\\_swan\\_2023/overview.htm](https://www.bis.org/events/green_swan_2023/overview.htm)



*Number 7***Responsible Cyber Power in Practice**

A Defence and Intelligence Partnership

Established in 2020, the National Cyber Force (NCF) is a partnership between GCHQ and the Ministry of Defence which carries out cyber operations on a daily basis to protect against threats to the UK, further the UK's foreign policy, support military operations, and prevent serious crime.



A Defence and Intelligence Partnership

**The National Cyber Force:****Responsible Cyber Power in Practice**

There are three broad categories of NCF operations:



Countering threats from terrorists, criminals and states using the internet to operate across borders in order to do harm in the UK and elsewhere.



Countering threats which undermine the confidentiality, integrity and availability of data, and effective use of systems by users. This can involve conducting cyber operations, when necessary, alongside the range of other mitigations available to counter threats to our cyber security, including improved cyber resilience, coordinated action with allied governments, and collaboration with the private sector.



Contributing to UK Defence operations and helping to deliver the UK's foreign policy agenda. Cyber operations can support the full range of Defence activity. And they can make a particular contribution in support of key foreign policy and security objectives.

## Licence to operate

The UK's approach to cyber operations has traditionally been kept highly secret. But this kind of work clearly prompts questions about how the UK can act in a responsible way that is consistent with its commitment to a free, open, peaceful and secure internet. With the creation of the NCF, and the degree of investment involved, it is right that we enable greater transparency and engage with the public more widely than has been done before. This document is part of that process. Doing so is a crucial part of assuring the force's 'licence to operate' in the public mind and demonstrating the UK's commitment to being a responsible and democratic cyber power. We do not take this for granted.

To read more:

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1148278/Responsible Cyber Power in Practice.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1148278/Responsible_Cyber_Power_in_Practice.pdf)





*Number 8***New Sensors With the HOTS for Extreme Missions**

Sensors are everywhere – except in harsh environments too hot for key components. DARPA’s new HOTS program looks to change that



Modern technologies are laden with sensors – a now-customary fact of life in much of the world. On smart watches and phones, and in cars and homes, sensors help monitor health, adjust various settings for comfort, and warn of potential dangers.

More widely, sensors are deployed across countless commercial and defense systems, including in the oil and gas sector, the automotive industry, alternative energy sources, geothermal applications, and aviation and aerospace.

In these broader industrial contexts, the capabilities of sensors can be inhibited by thermal limitations. A sensor may theoretically be able to process inputs such as speed, pressure, or the integrity of a mechanical component, but inside a turbine engine, temperatures far exceed what any existing sensor can withstand.

DARPA’s new High Operational Temperature Sensors (HOTS) program will work toward developing microelectronic sensor technologies capable of high-bandwidth, high-dynamic-range sensing at extreme temperatures.

“Many of the defense and industrial systems that rely on sensors experience harsh environments beyond the capability of today’s high-performance physical sensors. That means these systems have to be designed and operated with reduced performance and excessive margins – they’re limited by the uncertainty of their thermal environments,” said Dr. Benjamin Griffin, program manager for HOTS.

“However, if we can design, integrate, and demonstrate high-performance physical sensors that can operate in high-temperature environments, we can advance toward systems that perform at the edge of their capability instead of the limits of uncertainty.”

In development of next generation turbine engines or high-speed flight, thermal restrictions can hamstring progress.

For example, high-performance pressure sensors are needed to capture complex flow dynamics in extremely high temperature environments (i.e., 800 °C or 1472 °F).

Today, sensors that can withstand thermally harsh conditions are limited to low-sensitivity transducers located in hot zones coupled via noisy electrical connections to remote, temperature-constrained, silicon signal-conditioning microelectronics in cold zones.

The resulting integrated sensors lack the combination of frequency bandwidth and dynamic range essential for high-temperature missions.

Physical sensors that can overcome these limitations and optimally perform in high-temperature environments – without additional thermal management – will enable critical operations that include monitoring stability and functionality in extremely hot system components.

Combinations of emerging materials, fabrication techniques, and integration technologies that inform new types of transistors and transducers, are among the potential approaches the HOTS program hopes to demonstrate as a sensor module.

“If you look at the progress of cars alone, we’ve seen sort of a nervous system of sensing evolve, providing visibility and knowledge of what’s happening across the platform. Applying the same concept to larger-scale systems in harsh environments will offer tremendous benefits for the future system capabilities,” Griffin said.

HOTS will hold a Proposers Day on May 31, 2023. More information on the Proposers Day can be found [here](#). Further program details will be available in a forthcoming Broad Agency Announcement.

To read more: <https://www.darpa.mil/news-events/2023-05-12>



*Number 9*

## Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service



Through Operation MEDUSA, the FBI, and the U.S. Attorney's Office for the Eastern District of New York Neutralized the FSB's Premier Cyberespionage Malware Implant in Coordination with Multiple Foreign Governments.

The Justice Department announced the completion of a court-authorized operation, codenamed MEDUSA, to disrupt a global peer-to-peer network of computers compromised by sophisticated malware, called "Snake", that the United States Government attributes to a unit within Center 16 of the Federal Security Service of the Russian Federation (FSB).

For nearly 20 years, this unit, referred to in court documents as "Turla," has used versions of the Snake malware to steal sensitive documents from hundreds of computer systems in at least 50 countries, which have belonged to North Atlantic Treaty Organization (NATO) member governments, journalists, and other targets of interest to the Russian Federation.

After stealing these documents, Turla exfiltrated them through a covert network of unwitting Snake-compromised computers in the United States and around the world.

Operation MEDUSA disabled Turla's Snake malware on compromised computers through the use of an FBI-created tool named PERSEUS, which issued commands that caused the Snake malware to overwrite its own vital components.

Within the United States, the operation was executed by the FBI pursuant to a search warrant issued by United States Magistrate Judge Cheryl L. Pollak of the Eastern District of New York, which authorized remote access to the compromised computers.

This morning, the Court unsealed redacted versions of the affidavit submitted in support of the application for the search warrant, and of the search warrant issued by the Court.

For victims outside the United States, the FBI is engaging with local authorities to provide both notice of Snake infections within those authorities' countries and remediation guidance.

Merrick B. Garland, United States Attorney General; Breon Peace, United States Attorney for the Eastern District of New York; Lisa O. Monaco, Deputy Attorney General of the Justice Department; and Michael J. Driscoll, Assistant Director-in-Charge, FBI, New York Field Office, announced the operation.

“The Justice Department, together with our international partners, has dismantled a global network of malware-infected computers that the Russian government has used for nearly two decades to conduct cyber-espionage, including against our NATO allies,” stated Attorney General Garland.

“We will continue to strengthen our collective defenses against the Russian regime’s destabilizing efforts to undermine the security of the United States and our allies.”

“Russia used sophisticated malware to steal sensitive information from our allies, laundering it through a network of infected computers in the United States in a cynical attempt to conceal their crimes. Meeting the challenge of cyberespionage requires creativity and a willingness to use all lawful means to protect our nation and our allies,” stated United States Attorney Peace.

“The court-authorized remote search and remediation announced today demonstrates my Office and our partners’ commitment to using all of the tools at our disposal to protect the American people.”

“Through a high-tech operation that turned Russian malware against itself, U.S. law enforcement has neutralized one of Russia’s most sophisticated cyber-espionage tools, used for two decades to advance Russia’s authoritarian objectives,” stated Deputy Attorney General Monaco.

“By combining this action with the release of the information victims need to protect themselves, the Justice Department continues to put victims at the center of our cybercrime work and take the fight to malicious cyber actors.”

“The operation we announced today successfully disrupted the foremost cyber espionage tool of the Russian government. For two decades, the malware allowed Russian Intelligence to compromise computer systems and steal sensitive information - harming not only the United States Government and our allies but also private sector organizations.

This action should serve as a reminder to Russia and any other hostile nation willing to steal information, the FBI and our partners are united in our efforts to protect our countries,” stated FBI Assistant Director-in-Charge Driscoll.

“For 20 years, the FSB has relied on the Snake malware to conduct cyberespionage against the United States and our allies – that ends today,” said Assistant Attorney General Matthew G. Olsen of the Justice Department’s National Security Division.

“The Justice Department will use every weapon in our arsenal to combat Russia’s malicious cyber activity, including neutralizing malware through high-tech operations, making innovative use of legal authorities, and working with international allies and private sector partners to amplify our collective impact.”

As detailed in court documents, the U.S. government has been investigating Snake and Snake-related malware tools for nearly 20 years. The U.S. government has monitored FSB officers assigned to Turla conducting daily operations using Snake from a known FSB facility in Ryazan, Russia.

Although Snake has been the subject to several cybersecurity industry reports throughout its existence, Turla has applied numerous upgrades and revisions, and selectively deployed it, all to ensure that Snake remains the FSB’s most sophisticated long-term cyberespionage malware implant.

Unless disrupted, the Snake implant persists on a compromised computer’s system indefinitely, typically undetected by the machine’s owner or authorized users. The FBI has observed Snake persist on particular computers despite a victim’s efforts to remediate the compromise.

Snake provides its Turla operators the ability to remotely deploy selected malware tools to extend Snake’s functionality to identify and steal sensitive information and documents stored on a particular machine.

Most importantly, the worldwide collection of Snake-compromised computers acts as a covert peer-to-peer network, which utilizes customized communication protocols designed to hamper detection, monitoring, and collection efforts by Western and other signals intelligence services.

Turla uses the Snake network to route data exfiltrated from target systems through numerous relay nodes scattered around the world back to Turla operators in Russia. For example, the FBI, its partners in the U.S. Intelligence Community, together with allied foreign governments, have monitored the FSB’s use of the Snake network to exfiltrate data from

sensitive computer systems, including those operated by NATO member governments, by routing the transmission of these stolen data through unwitting Snake-compromised computers in the United States.

As described in court documents, through analysis of the Snake malware and the Snake network, the FBI developed the capability to decrypt and decode Snake communications.

With information gleaned from monitoring the Snake network and analyzing Snake malware, the FBI developed a tool, named PERSEUS, that establishes communication sessions with the Snake malware implant on a particular computer, and issues commands that causes the Snake implant to disable itself without affecting the host computer or legitimate applications on the computer.

Today, to empower network defenders worldwide, the FBI, the National Security Agency, the Cybersecurity and Infrastructure Security Agency, the U.S. Cyber Command Cyber National Mission Force, and six other intelligence and cybersecurity agencies from each of the Five Eyes member nations, issued a joint cybersecurity advisory (the “Joint Advisory”) with detailed technical information about the Snake malware that will allow cybersecurity professionals to detect and remediate Snake malware infections on their networks.

The Joint Advisory is available [here](#). The FBI and U.S. Department of State are also providing additional information to local authorities in countries where computers that have been targeted by the Snake malware have been located.

Although Operation MEDUSA disabled the Snake malware on compromised computers, victims should take additional steps to protect themselves from further harm.

The operation to disable Snake did not patch any vulnerabilities or search for or remove any additional malware or hacking tools that hacking groups may have placed on victim networks.

The Department of Justice strongly encourages network defenders to review the Joint Advisory for further guidance on detection and patching.

Moreover, as noted in court documents, Turla frequently deploys a “keylogger” with Snake that Turla can use to steal account authentication credentials, such as usernames and passwords, from legitimate users. Victims should be aware that Turla could use these stolen credentials to fraudulently re-access compromised computers and other accounts.



The FBI has is providing notice of the court-authorized operation to all owners or operators of the computers remotely accessed pursuant to the search warrant.

The criminal investigation into the FSB's use of the Snake malware is being handled by the Office's National Security and Cybercrime Section. Assistant United States Attorney Ian C. Richardson is in charge of the investigation, with assistance from the National Security Division's Counterintelligence and Export Control Section.

The efforts to disrupt the Snake malware network were led by the FBI's New York Field Office, FBI's Cyber Division, the U.S. Attorney's Office for the Eastern District of New York, and the National Security Division's Counterintelligence and Export Control Section. Assistance was also provided by the Criminal Division's Computer Crime and Intellectual Property Section.

Those efforts would not have been successful without the partnership of numerous private-sector entities, including those victims who allowed the FBI to monitor Snake communications on their systems.

To read more:

<https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network>



*Number 10***Hunting Russian Intelligence “Snake” Malware**

The Snake implant is considered the most sophisticated cyber espionage tool designed and used by Center 16 of Russia’s Federal Security Service (FSB) for long-term intelligence collection on sensitive targets.

To conduct operations using this tool, the FSB created a covert peer-to-peer (P2P) network of numerous Snake-infected computers worldwide.

Many systems in this P2P network serve as relay nodes which route disguised operational traffic to and from Snake implants on the FSB’s ultimate targets.

Snake’s custom communications protocols employ encryption and fragmentation for confidentiality and are designed to hamper detection and collection efforts.

We have identified Snake infrastructure in over 50 countries across North America, South America, Europe, Africa, Asia, and Australia, to include the United States and Russia itself.

Although Snake uses infrastructure across all industries, its targeting is purposeful and tactical in nature.

Globally, the FSB has used Snake to collect sensitive intelligence from high-priority targets, such as government networks, research facilities, and journalists.

As one example, FSB actors used Snake to access and exfiltrate sensitive international relations documents, as well as other diplomatic communications, from a victim in a North Atlantic Treaty Organization (NATO) country.

Within the United States, the FSB has victimized industries including education, small businesses, and media organizations, as well as critical infrastructure sectors including government facilities, financial services, critical manufacturing, and communications.

This Cybersecurity Advisory (CSA) provides background on Snake’s attribution to the FSB and detailed technical descriptions of the implant’s

host architecture and network communications. This CSA also addresses a recent Snake variant that has not yet been widely disclosed.

The technical information and mitigation recommendations in this CSA are provided to assist network defenders in detecting Snake and associated activity.

For more information on FSB and Russian state-sponsored cyber activity, please see the joint advisory Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure and CISA's Russia Cyber Threat Overview and Advisories webpage.

You may visit:

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a>

<https://www.cisa.gov/russia>



## Russia Cyber Threat Overview and Advisories



This page provides an overview of the Cybersecurity and Infrastructure Security Agency's (CISA's) assessment of the Russian government's malicious cyber activities. The overview leverages publicly available, open-source intelligence and information

regarding this threat. This page also includes [a complete list of related CISA publications](#), many of which are jointly authored with other U.S. government agencies

### TABLE OF CONTENTS

Summary .....	1
Introduction .....	4
What is Snake? .....	4
Background .....	4
Attribution .....	5
Victimization .....	5
Other Tools and TTPs Employed with Snake .....	6
Snake Architecture .....	6
Capitalizing on Mistakes .....	7

Snake Host-Based Technical Details.....	8
Installer.....	8
On-Disk Components.....	8
The Queue.....	11
Snake Network Communications.....	17
Network Obfuscation.....	17
Snake's Network Authentication Technique ("ustart").....	17
Snake UDP.....	19
Snake HTTP.....	20
Snake TCP.....	21
Snake "enc" Layer.....	23

To read more:

[https://www.cisa.gov/sites/default/files/2023-05/aa23-129a\\_snake\\_malware\\_1.pdf](https://www.cisa.gov/sites/default/files/2023-05/aa23-129a_snake_malware_1.pdf)



## Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any individual or entity;
- should not be relied on in the context of enforcement or similar regulatory action;
- is not necessarily comprehensive, complete, or up to date;
- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;
- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);
- is in no way constitutive of an interpretative document;
- does not prejudice the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;
- does not prejudice the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors.

However, some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility regarding such problems incurred because of using this site or any linked external sites.

## International Association of Risk and Compliance Professionals (IARCP)

You can explore what we offer to our members:



1. *Membership* – Become a standard, premium or lifetime member.

You may visit:

[https://www.risk-compliance-association.com/How to become member .htm](https://www.risk-compliance-association.com/How_to_become_member.htm)

2. *Weekly Updates* - Visit the *Reading Room* of the association at: [https://www.risk-compliance-association.com/Reading Room.htm](https://www.risk-compliance-association.com/Reading_Room.htm)

3. *Training and Certification* – Become:

- a Certified Risk and Compliance Management Professional (CRCMP),
- a Certified Information Systems Risk and Compliance Professional (CISRCP),
- a Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P,
- a Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I,
- a Travel Security Trained Professional (TSecTPro).

The CRCMP has become one of the most recognized certificates in risk management and compliance. There are CRCMPs in 32 countries.

Companies and organizations around the world consider the CRCMP a preferred certificate:

### Senior Information Security Risk Analyst

Public Company Accounting Oversight Board - ★★★★★ 10 reviews - Washington, DC

Professional designation in CISSP, CISA, CRISC, or CRCMP preferred. The PCAOB is a nonprofit corporation established by Congress to oversee the audits of public...



www.simplyhired.com/search?q=crcmp&job=BY\_s7GxAbt4KwSJ\_aJA\_4KaruYRQSQ





## Crcmp jobs

Sort by

Date Added

More Filters

Relevance ▾

Anytime ▾

None Selected ▾

### Risk Science Business Process Lead, Senior Associate

Capital One - McLean, VA

Est. \$110,000 - \$150,000 a year ⓘ

Lean, Six Sigma, BPM, PMP, PRM, or CRCMP. McLean 1 (19050), United States of America, McLean, Virginia....

### Application Security Advisor-Penetration Tester

USAA - San Antonio, TX

Est. \$100,000 - \$140,000 a year ⓘ

Professional designation in CISSP, CISA, CRISC, CISM, CEH, GWAPT, GWEB, or CRCMP. Purpose of Job IMPORTANT:....



### Senior Manager Vendor Risk Management

Johnson & Johnson Family of Companies ★★★★★ 3,153 reviews -

New Brunswick, NJ

[Apply On Company Site](#)

requirements.

- Stay abreast of regulatory environment regarding VRM.

#### Qualifications

- A minimum of a Bachelor's degree or equivalent is required.
- Compliance Certification (CRCMP) designation is preferred.
- A minimum of 6 years experience in IT compliance, finance compliance and/or payroll compliance is required.
- Experience leading & executing SOX 404 compliance programs is required.
- Prior experience with vendor risk management preferred.
- Experience working with 3rd party vendors is preferred.

You can find more about the demand for CRCMPs at:

[https://www.risk-compliance-association.com/CRCMP\\_Jobs\\_Careers.pdf](https://www.risk-compliance-association.com/CRCMP_Jobs_Careers.pdf)

For the Certified Risk and Compliance Management Professional (CRCMP) distance learning and online certification program, you may visit:

[https://www.risk-compliance-association.com/Distance\\_Learning\\_and\\_Certification.htm](https://www.risk-compliance-association.com/Distance_Learning_and_Certification.htm)

For the Certified Information Systems Risk and Compliance Professional (CISRCP), distance learning and online certification program, you may visit:

[https://www.risk-compliance-association.com/CISRCP\\_Distance\\_Learning\\_and\\_Certification.htm](https://www.risk-compliance-association.com/CISRCP_Distance_Learning_and_Certification.htm)

For the Certified Cyber (Governance Risk and Compliance) Professional - CC(GRC)P, distance learning and online certification program, you may visit:

[https://www.risk-compliance-association.com/CC\\_GRC\\_P\\_Distance\\_Learning\\_and\\_Certification.htm](https://www.risk-compliance-association.com/CC_GRC_P_Distance_Learning_and_Certification.htm)

For the Certified Risk and Compliance Management Professional in Insurance and Reinsurance - CRCMP(Re)I distance learning and online certification program, you may visit:

[https://www.risk-compliance-association.com/CRCMP\\_Re\\_I.htm](https://www.risk-compliance-association.com/CRCMP_Re_I.htm)

For the Travel Security Trained Professional (TSecTPro), distance learning and online certification program, you may visit:

[https://www.risk-compliance-association.com/TSecTPro\\_Distance\\_Learning\\_and\\_Certification.htm](https://www.risk-compliance-association.com/TSecTPro_Distance_Learning_and_Certification.htm)

Certified Cyber (Governance Risk and Compliance) Professionals - CC(GRC)Ps, have a 50% discount for the Travel Security Trained Professional (TSecTPro) program (\$148 instead of \$297).

You have a \$100 discount after you purchase one of our programs. The discount applies to each additional program. For example, you can purchase the CRCMP program for \$297, and then purchase the CISRCP program for \$197 (instead of \$297), the CC(GRC)P program for \$197 (instead of \$297), the CRCMP(Re)I program for \$197 (instead of \$297), and the TSecTPro program for \$197 (instead of \$297).

For *instructor-led* training, you may contact us. We can tailor all programs to meet specific requirements.